Délibération n° 2017-079 du 17 mai 2017

de la Commission de Contrôle des Informations Nominatives portant autorisation à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Sécurité et contrôle d'accès aux locaux par badge non biométrique* »

présenté par la BNP Paribas Wealth Management Monaco

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu la délibération n° 2010-43 du 15 novembre 2010 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les dispositifs de contrôle d'accès sur le lieu de travail mis en œuvre par les personnes physiques ou morales de droit privé ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par la BNP Paribas Wealth Management Monaco le 13 février 2017, concernant la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité « *Sécurité et contrôle d'accès aux locaux par badge non biométrique* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 11 avril 2017, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 mai 2017 portant examen du traitement automatisé susvisé.

## La Commission de Contrôle des Informations Nominatives,

### Préambule

BNP Paribas Wealth Management Monaco est une société monégasque, immatriculée au Répertoire du Commerce et de l'Industrie sous le numéro 91S02724, ayant entre autres pour objet « *en Principauté de Monaco et à l'étranger pour son compte ou le compte de tiers, directement ou en participation : La réalisation de toutes opérations de banque ou connexes telles que définies par la « loi bancaire » applicable (… )*».

Afin d'assurer la sécurité des biens et des personnes ainsi que la confidentialité des données détenues, le responsable de traitement souhaite procéder à l'installation d'un système de contrôle d'accès par badge non biométrique au sein de son établissement.

Le traitement objet de la présente demande est mis en œuvre à des fins de surveillance. Il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

### I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « Sécurité et *contrôle d'accès aux locaux par badge non biométrique* ».

Le responsable de traitement indique que les personnes concernées sont « *les employés, auditeurs externes et prestataires externes, sous-traitants permanents* ».

Enfin, les fonctionnalités du traitement sont les suivantes :

- « *Assurer la sécurité des personnes et des biens par ségrégation des accès entre les clients et le personnel et les intervenants extérieurs ;*
- *Assurer la sécurité des personnes et des biens en contrôlant les accès aux locaux identifiés comme sensibles bénéficiant d'une circulation limitée ;*
- *Gérer les habilitations d'accès aux personnes autorisées ;*
- *Désactiver les badges perdus/volés ;*
- *Permettre la constitution de preuve en cas d'infraction* ».

La Commission constate que la finalité du traitement est explicite et légitime, conformément à l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

### II. Sur la licéité et la justification du traitement

Dans le cadre de ses activités, BNP Paribas Wealth Management Monaco est amenée à exploiter des données pour le compte de ses clients, et notamment des données relatives aux activités bancaires.

A cet égard, la Commission constate que ce système de contrôle d'accès est justifié par la réalisation d'un intérêt légitime du responsable de traitement puisqu'il permet d'assurer « *la protection des personnes et des biens ainsi qu'assurer la confidentialité des données détenues grâce à une restriction d'accès aux locaux aux seules personnes dûment habilitées ».*

Par ailleurs, elle prend acte des précisions du responsable de traitement selon lesquelles ce système « *ne méconnait pas les droits et libertés fondamentaux des personnes concernées »* puisque celles-ci « *bénéficient d'une information préalable et suffisante sur son existence et son exploitation* » et que ce traitement *« n'a pas pour objet de contrôler de manière inopportune les comportements, les habitudes et les horaires des personnes concernées ».*

Au vu de ce qui précède, la Commission considère que le traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

## III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : employés/ tiers (auditeurs externes, prestataires, sous-traitants permanents) : nom société, nom, prénom ;
- formation - diplômes - vie professionnelle : famille d'accès, plages horaires spécifiques ;
- badge : numéro d'antenne (référence badge), date de délivrance, état (activé ou désactivé) ;
- informations relatives à la vie professionnelle : plage horaire spécifique ;
- horodatage : horodatage des accès aux locaux : nom, prénom, nom du point de passage, autorisé (oui/non), date, heure.

S'agissant du personnel, les informations relatives à l'identité, la formation, les diplômes, la vie professionnelle et les badges ont pour origine le traitement légalement mis en œuvre « *Gestion administrative des salariés* ».

S'agissant des auditeurs externes, des prestataires permanents et sous-traitants, les informations relatives à l'identité, la formation, les diplômes, la vie professionnelle et les badges ont pour origine les contrats ou les lettres de mission les liant au responsable de traitement.

Les informations relatives à l'horodatage sont générées par le système lui-même.

La Commission relève de plus que les logs de connexion des personnes habilitées à avoir accès au traitement générés par le système, sont également collectés.

Au vu de ce qui précède, la Commission considère que les informations traitées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

## IV. Sur les droits des personnes concernées

- ***Sur l'information des personnes concernées***

Le responsable de traitement indique que l'information préalable des personnes concernées est effectuée comme suit :

- pour les employés, par le biais d'un formulaire de délivrance de badge et d'une procédure « Informations Nominatives » accessible sur l'Intranet de la banque ;

- pour les tiers (auditeurs externes et prestataires externes, sous-traitants permanents), par le biais d'un formulaire de délivrance de badge.

La Commission considère, à la lecture des documents qui ont été joints, qu'ils ne comportent pas l'ensemble des mentions prévues par l'article 14 de la Loi n°1.165 du 23 décembre 1993.

En conséquence, la Commission demande que l'information préalable des personnes concernées soit assurée conformément à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

- ***Sur l'exercice du droit d'accès des personnes concernées***

Le droit d'accès s'exerce par voie postale auprès du Chief Operating Officer (COO) pour les employés et auprès du service réclamation pour les auditeurs et prestataires externes et sous-traitants permanents.

La réponse à ce droit d'accès s'exerce selon les mêmes modalités dans un délai de 30 jours.

La Commission considère que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

## V. Sur les destinataires et les personnes ayant accès au traitement

- ***Sur les destinataires***

Les informations sont susceptibles d'être communiquées aux Autorités Policières et Judiciaires légalement habilitées.

La Commission estime que ces communications peuvent être justifiées pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, lesdites Autorités ne pourront avoir communication des informations que dans le strict cadre de leurs missions légalement conférées.

La Commission considère que ces transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Les personnes ayant accès au traitement sont :

- les membres de l'administration générale (correspondants sécurité) : tous droits ;
- le service contrôle interne : consultation ;
- le prestataire de service : tous droits pour la maintenance sous la supervision d'un personnel habilité de la banque.

Considérant les attributions de chacune de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

En ce qui concerne le prestataire, la Commission rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 ses droits d'accès doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, aux termes de ce même article.

Elle rappelle enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993, la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

## VI. Sur les rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet d'un rapprochement avec le traitement ayant pour finalité « *Gestion administrative des salariés* ».

A cet égard, la Commission constate que ce traitement a été légalement mis en œuvre.

## VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

La Commission rappelle également que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

Elle constate que la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

## VIII. Sur la durée de conservation

Les informations relatives à l'identité, la formation, les diplômes, la vie professionnelle et les badges sont conservées 5 ans après la fin du contrat de travail pour les employés et un mois après la fin de mission pour les auditeurs externes, prestataires ou sous-traitants permanents.

Les informations relatives à l'horodatage sont conservées un mois.

S'agissant des logs de connexion la Commission rappelle qu'ils doivent être conservés entre 3 mois et 1 an.

La Commission considère que ces durées de conservation sont conformes aux exigences légales.

**Après en avoir délibéré, la Commission :**

**Constate que** la copie ou l'extraction d'informations issues de ce traitement est chiffrée sur son support de réception.

**Rappelle que :**

- les Autorités Policières et Judiciaires ne pourront avoir communication des informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;

- les logs de connexion doivent être conservés entre 3 mois et 1 an ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare feux) ainsi que les comptes utilisateurs et administrateurs doivent être protégés nominativement par un identifiant et un mot de passe réputé fort.

**Demande que** l'information préalable des personnes concernées comporte l'ensemble des mentions prévues par l'article 14 de la Loi n°1.165 du 23 décembre 1993.

**A la condition de la prise en compte de ce qui précède,**

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par BNP Paribas Wealth Management Monaco du traitement automatisé d'informations nominatives ayant pour finalité « *Sécurité et contrôle d'accès aux locaux par badge non biométrique* ».**

Le Président

Guy MAGNAN